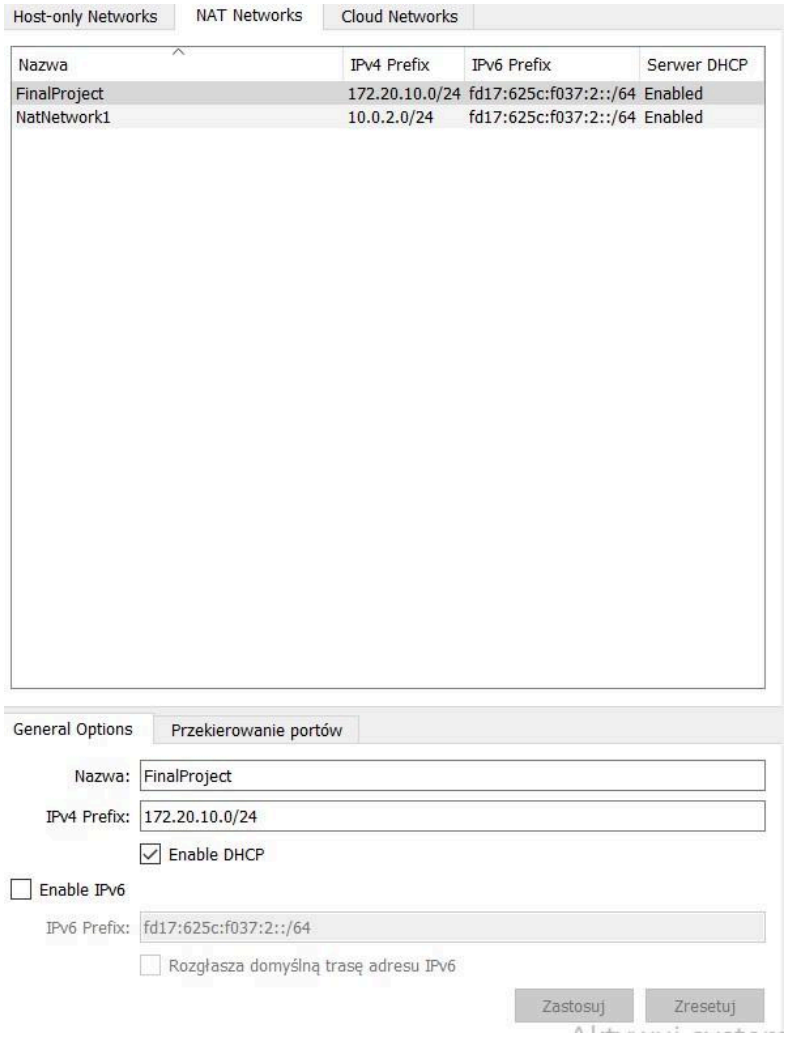
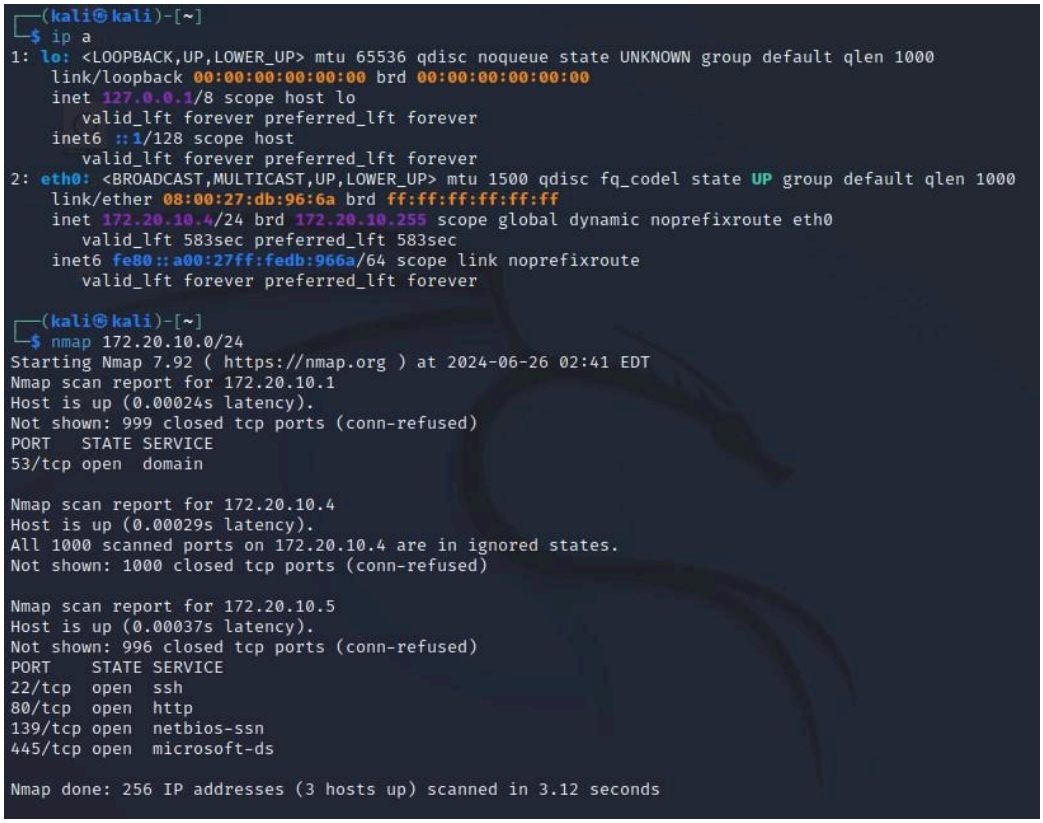
Bypassing the perimeter final project
Kacper Waliczek

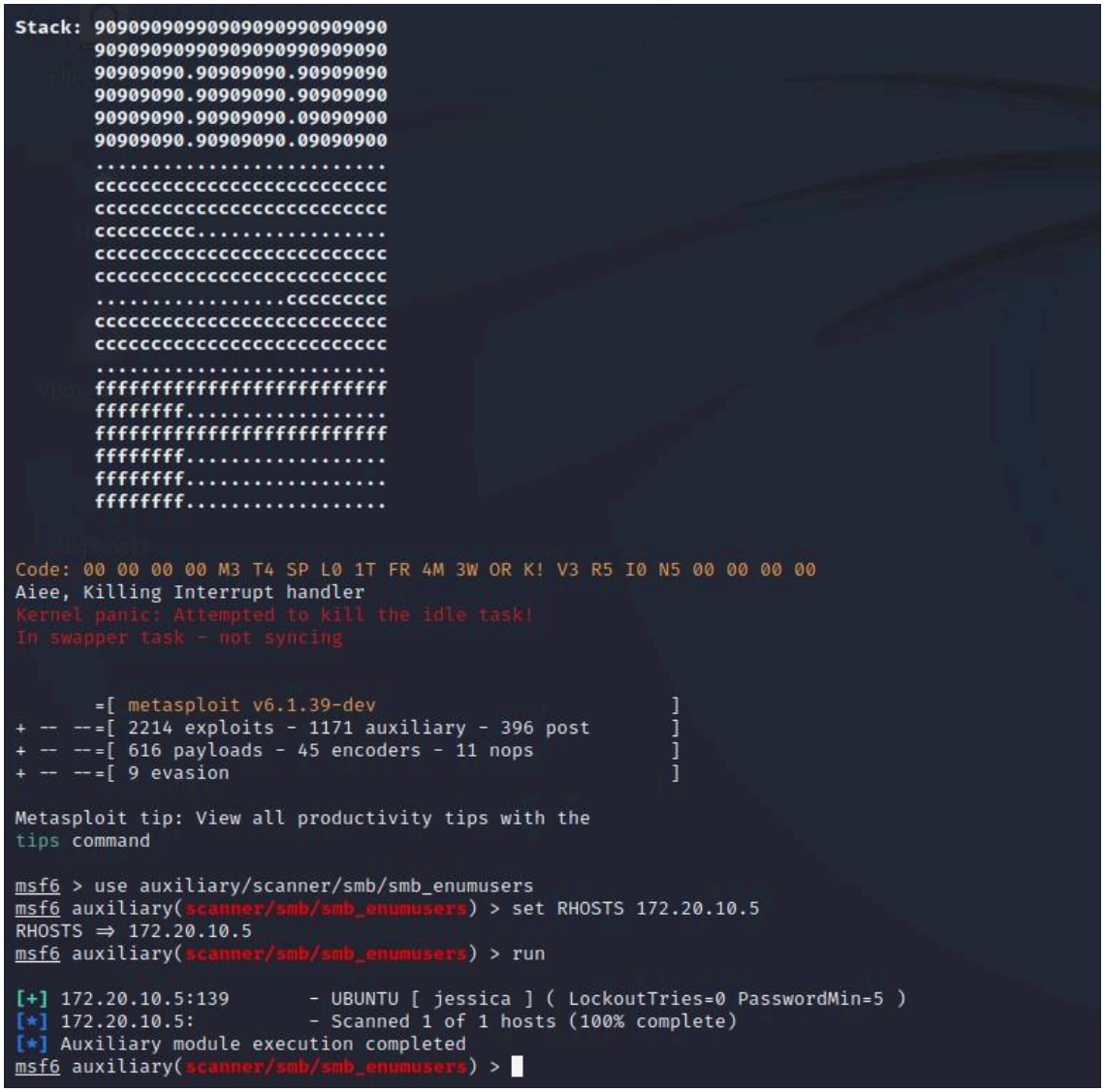
Setting ip in Nat Network



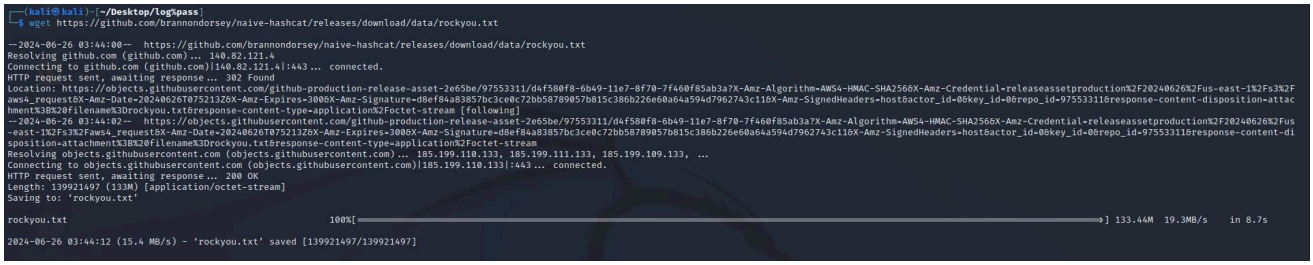
1. Nmap

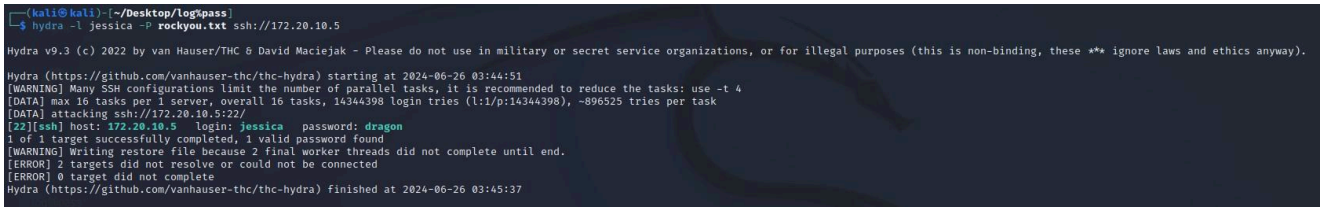

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:db:96:6a brd ff:ff:ff:ff:ff:ff
inet 172.20.10.4/24 brd 172.20.10.255 scope global dynamic noprefixroute eth0
valid_lft 583sec preferred_lft 583sec
inet6 fe80::a00:27ff:fedb:966a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
┌──(kali㉿kali)-[~]
└─$ nmap 172.20.10.0/24
Starting Nmap 7.92 (https://nmap.org) at 2024-06-26 02:41 EDT
Nmap scan report for 172.20.10.1
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT STATE SERVICE
53/tcp open domain
Nmap scan report for 172.20.10.4
Host is up (0.00029s latency).
All 1000 scanned ports on 172.20.10.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)
Nmap scan report for 172.20.10.5
Host is up (0.00037s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.12 seconds

2. Metasploit

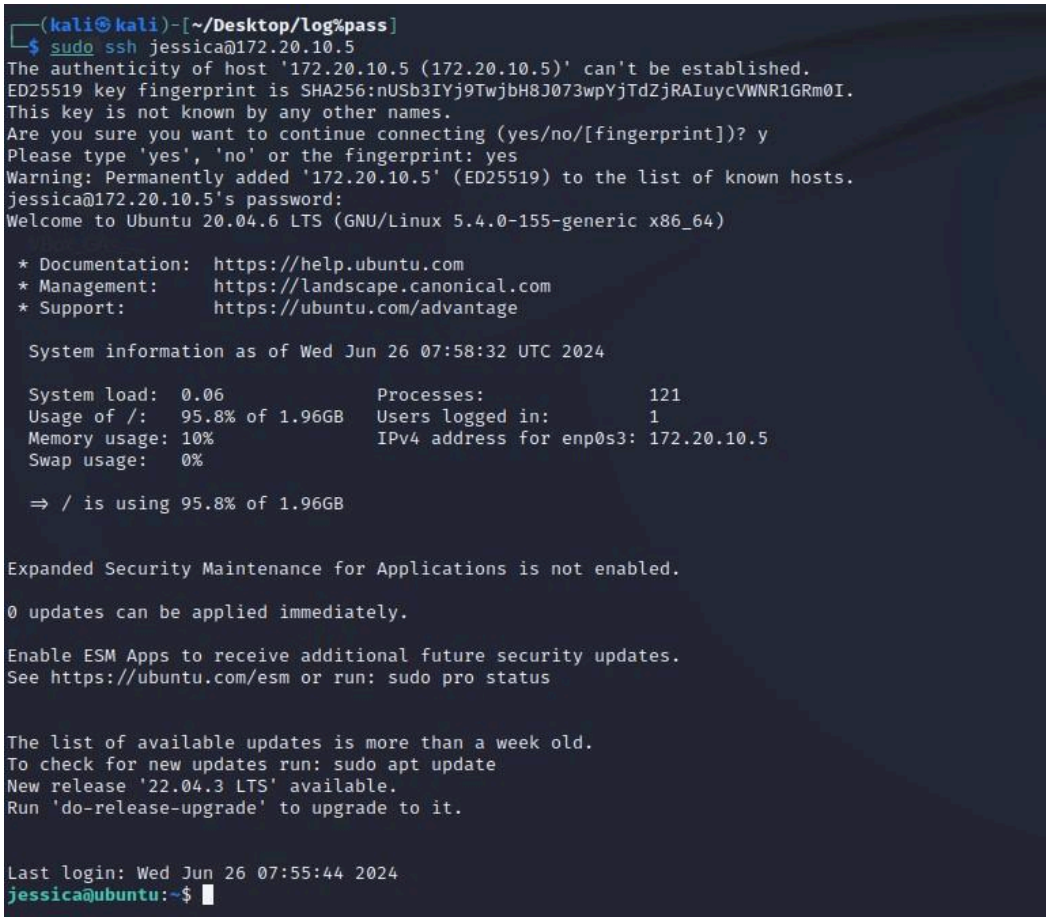


3. Downloading rockyou.txt from Github & Hydra

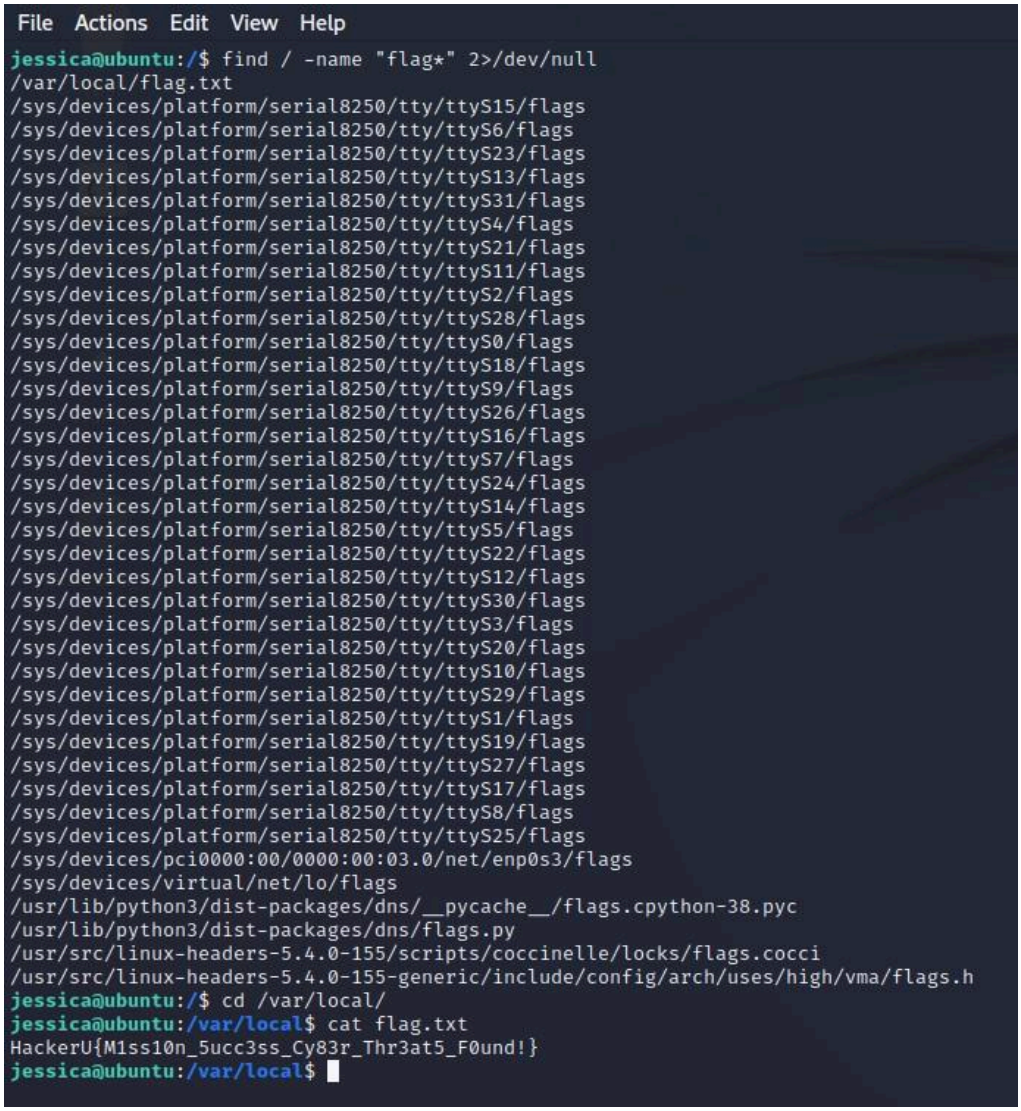




4. Login to jessica@172.20.10.5 via SSH



5. Searching for flag



Flag: HackerU{M1ss10n_5ucc3ss_Cy83r_Thr3at5_F0und!}